Dell EMC Converged Systems Upgrade Guide

from VMware vSphere 6.0 or VMware vSphere 6.5 to VMware vSphere 6.7

D&LL Technologies

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

⚠ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

Contents

Revision history

Date	Document revision	Description of changes
April 2021	1.4	Updated the note in *Hardware, software, and license* requirement for Cisco UCS M3 rack servers, VxBlock System 240, and VMware vSphere 6.7.
May 2020	1.3	Updated the note in *Hardware, software, and license* requirement for Cisco UCS M3 rack servers and vSphere 6.7.
September 2019	1.2	Added support for VMware NSX. Added information about External and Embedded PSCs. Modified the section *Part III - Upgrading to VMware vSphere 6.7 > Upgrade recommendations* .
June 2019	1.1	Added support for VxBlock System 240 and VxBlock System 340.
March 2019	1.0	Initial release

Introduction

Use this guide to upgrade Converged Systems from RCM releases that support VMware vSphere 6.0 and VMware vSphere 6.5 to an RCM release that supports VMware vSphere 6.7. This document also provides prerequisites and strategies to minimize system downtime.

See the RCM Portal on the Dell EMC Technical Resource Center for supported RCM releases for the Converged Systems. (requires log in)

This upgrade procedure is for Converged Systems that include the VMware vSphere Distributed Switch (VDS).

The target audience for this document includes build teams, deployment and installation personnel, sales engineers, field consultants, advanced services specialists, and customers. Use these instructions to upgrade the following Converged Systems:

- VxBlock System 240
- VxBlock System 340
- VxBlock System 350
- VxBlock System 540
- VxBlock System 740
- VxBlock System 1000

See the following table for information about other upgrade instructions:

To upgrade this product	See this document
AMP-3S	*Dell EMC AMP-3S Software and Firmware Upgrade Guide*
VMware vSphere 6.5 to 6.7	*Dell EMC Upgrade Guide from VMware vSphere 6.0 or VMware vSphere 6.5 to VMware vSphere 6.7*
Cisco DCNM	*Dell EMC Converged Systems Upgrade Guide from Cisco DCNM 7.2 to Cisco DCNM 10.x*
Vision™ Intelligent Operations	*Dell EMC Vision™ Intelligent Operations Upgrade Guide*
One RCM release to another within the same RCM train, for example, upgrading from RCM release 6.5.x to the next 6.5.x release.	Dell EMC upgrade guide for the Converged System you need to upgrade
VxBlock Central	*Dell EMC VxBlock Central Upgrade Guide*

(i) **NOTE:** In this document, all upgrades are on AMP-2V, AMP-2P, AMP-2S, AMP-3S, and AMP-VX.

(i) **NOTE:** Starting with VMware vSphere 6.5, the Cisco Nexus 1000V is not supported. Dell EMC recommends migrating from the Cisco Nexus 1000V switch to the VMware Virtual Distributed Switch (VDS) before upgrading to vSphere 6.7.

The Glossary provides terms, definitions, and acronyms.

Part I - Upgrade prerequisites

Hardware, software, and license requirements

This section explains the hardware, software, and license requirements for upgrading to VMware vSphere 6.7.

Before upgrading a Converged System to VMware vSphere 6.7, review the following:

- For the upgrade to VMware vCenter Server Appliance (vCSA) components, one temporary IP address is required. If the Platform Services Controller (PSC) is migrating from embedded to external, it requires two more permanent IP addresses. The temporary IP address must be on the same subnet as the VMware vCenter Server and accessible by the current VMware vCenter Server environment. This temporary IP address is required to migrate configuration and services data from:
  - VMware vCenter Server 6.0 or 6.5 PSC
  - VMware vCenter Server 6.0 for Windows
  - vCSA 6.0 or 6.5 to vCSA 6.7
- Vblock Systems must migrate from an environment using Cisco Nexus 1000V virtual switch to an environment using VMware VDS. Contact Customer Support to migrate from the Cisco Nexus 1000V to VMware VDS.
- For compute Cisco UCS B- and C-Series Servers, Dell EMC recommends a boot LUN size of 15 GB to facilitate VMware vSphere ESXi core dumps. See the Administration Guide associated with your Converged System to extend the size of the LUN from 10 GB – 15 GB.
- IPv6 is not supported with VMware vSphere ESXi 6.7 on AMP-VX with vSAN and vSphere HA enabled.
- (i) **NOTE:**

  For VMware vSphere 6.7, the following Cisco UCS servers are supported:

  - Standalone Cisco IMC-managed Cisco UCS C2xx M4 rack servers or higher
  - Cisco UCSM-managed Cisco UCS C2xx M3 rack and blade servers or higher

  For VMware vSphere 6.7 U3 only, standalone Cisco IMC-managed Cisco UCS C2xx M3 rack servers or higher are supported as AMP servers.

  Starting with VMware vSphere 6.7, Cisco UCS M3 rack-mount servers are no longer used as Production servers on the VxBlock System 240. Plan hardware and server upgrades accordingly.

  See the VMware Compatibility Guide for more information.
- Verify that the firmware version of the Cisco UCS B and C-Series servers in your Converged System is compatible with VMware vSphere 6.7. See the *Converged System Release Certification Matrix* and the *Converged System Release Notes* for the release to which you are upgrading for more information.
- When upgrading to vSphere 6.7, evaluate the active/consumed memory and ensure to have enough physical memory on the AMP hosts.
- Ensure that you review and comply with the license requirements as specified in the Release Notes for the release of the software on your Converged System.
- Verify that the new vCSA and PSC meet the hardware requirements, including the additional required disk storage and memory. See the System Requirements section of the VMware vSphere Upgrade documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-752FCA83-1A9B-499E-9C65-D5625351C0B5.html
- Verify that all components are in a ready state and free from errors and alarms.
- Verify that Vision Intelligent Operations is at version 3.6.2 or higher. If you must upgrade, see the appropriate *Vision Intelligent Operations Upgrade Guide* or *Dell EMC VxBlock™ Central Upgrade Guide.*
- If the environment has VMware NSX, upgrade to VMware NSX 6.4.x before upgrading VMware vCenter Server to 6.5. VMware NSX 6.2.x is incompatible with VMware vCenter Server 6.5 but is compatible with NSX 6.4. See the *Dell EMC Converged Systems Upgrade Guide from VMware NSX 6.2.x to VMware NSX 6.4.x* for VMware NSX upgrade procedures. See the VMware compatibility Matrix for compatibility between NSX and vSphere: http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&2=2332,2136&93=2349,2528,2436

> **NOTE:** On VMware vSphere 6.7 deployments, disable the Host TPM attestation alarm definition to suppress attestation errors when TPM modules are installed but not used.

The recommendation is to increase Max LUN value for Fibre Channel Adapter policy to 1024. To increase the MAX LUN:

1. In UCSM, select **SAN** > **Policies** > **root** > **Fibre Channel Adapter Policies**.
2. Select the adapter policy of the ESXi hosts.
3. Select **Options**.
4. Set the **MAX LUN per Target** to **1024**.

   > **NOTE:** Updating the MAX LUN may cause traffic disruption for all hosts, so update the MAX LUN before upgrading to ESXi 6.7.

5. After upgrading to ESXi 6.7, log in to vCenter using the HTML5 client.
6. Select **Host** > **Manage** > **Advanced System Settings** > **Edit**.
7. In **Filter type**, set the **disk.maxLUN** to **1024** for each host.

Upgrade best practices

Follow the upgrade best practices to ensure minimum impact on the production traffic.

Use the following guidelines as you prepare for the upgrade:

- Refer to the best practices for upgrading to VMware vCenter Server 6.7: https://kb.vmware.com/s/article/54008
- Plan and prepare for the VMware vSphere 6.7 upgrade to ensure minimum impact on production traffic.
- Review this entire guide and each referenced document before you begin the upgrade.
- Follow the practices of your company for performing upgrades. If possible, perform the upgrade during a scheduled maintenance windows.
- Schedule adequate downtime for system maintenance. Downtime applies to all virtual infrastructure hosts and servers, including the virtual machines (VMs) that are running in the environment. Power down the VMs before upgrading to the latest recommended virtual hardware version. Also, you may need to restart VMs after completing the VMware Tools upgrade.
- For a VxBlock System with AMP-2V running with the production workload, plan and prepare for the upgrade to ensure minimum impact to production workload.
- For components in a cluster configuration, upgrade and verify the subordinate component before you upgrade the primary component. After you successfully upgrade the subordinate and primary components, verify the status of the components again to ensure that there are no new alarms.
- Do not change the system configuration during the upgrade.
- Check that network time protocol (NTP) is properly configured and functioning on all upgrade-related components or services. Ensure that clocks (time, time zone, and dates) on all hosts and that AMP VMs are synchronized before beginning the upgrade.
- Verify that Domain Name Service (DNS) (including type A and PTR records) and any local hosts files are properly configured for all upgrade-related components or services.
- Verify that the domain user account has the following permissions if the operating system is joined to the Active Directory domain:
  - Is a member of the Administrators group
  - Acts as part of the operating system
  - Logs in as a service
- Verify that the **Network Service** account has read permission on the folder in which VMware vCenter Server is installed and on the HKEY_LOCAL_MACHINE (HKLM) registry.
- Verify that the connection between the host machine and the domain controller is working.
- When upgrading the VNXe software used for management, check the lockdown status on all management ESXi servers. If the lockdown status is enabled, disable it before upgrading and enable it after upgrading.
- Keep AMP-VX and VxBlock 1000 on same RCM version.
- Verify that the SSO and operating system do not have the same root password.
- You do not need to break the partnership between PSCs to upgrade the Enhanced Link Mode (ELM) configuration.

Required skills

Basic knowledge around Converged Systems, VMs and Microsoft Windows administration are required.

To perform the upgrade, you should understand Microsoft Windows administration of the system architecture and technical skills and VM technology and data center operations. Be familiar with Converged Systems concepts, terminology, and troubleshooting.

If there is a question regarding ability and skills, contact Software Deployment Services (SDS) to perform the upgrade.

Besides these skills, you must:

- Have a computer with network access to the Converged Systems and the management systems.
- Understand the entire upgrade process before you upgrade the Converged Systems.

Part II - Pre-upgrade tasks

Download VMware vSphere files for upgrade

Download the files needed to upgrade to VMware vSphere 6.7. Each item is listed in the Converged System RCM 6.7.

Download the following files on a Converged System from the Flexera Download Center:

- VMware vCenter Server Appliance 6.7 ISO
- Dell EMC Custom ESXi 6.7 ISOs (AMP and compute)

ⓘ **NOTE:** For AMP Management VMware vSphere ESXi hosts only, ensure that the image does not contain PowerPath modules.

Back up the system and hosts

Follow this procedure for the order in which you should back up Converged Systems and hosts.

Steps

1. Back up the Converged System configuration and hosts.

   See the appropriate Administration Guide for instructions. Follow the backup procedures for your organizations.

2. Back up the VMware vCenter Server database on the AMP.
   - For Microsoft Windows with SQL database, use the procedure in the KB article: https://kb.vmware.com/s/article/2012138
   - For vCSA 6.0 or 6.5, use the procedure in the KB article: https://kb.vmware.com/s/article/2091961

3. Back up the PSCs.

   See the following for the procedure:
   - For vSphere 6.0, see https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-9AD16C4E-FCC1-4EFA-83D1-049B21B53876.html.
   - For vSphere 6.5, see https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.install.doc/GUID-8C9D5260-291C-44EB-A79C-BFFF506F2216.html.

4. Back up vCSA 6.0 or 6.5 certificates on the AMP. For Windows using external SSL certificates, make a copy of the SSL folder. The default path is C:\ProgramData\VMware\VMware VirtualCenter.

5. Visually inspect all hardware components to verify that there are no visible faults (amber lights). All components should be in the ready state and free from errors and alarms.

   ⓘ **NOTE:** Clone the management VMs during the maintenance window.

6. If you have an NSX environment, back up the NSX manager and the configuration of each VDS.

   See *NSX Backup and Restore*.

   https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/com.vmware.nsx.upgrade.doc/GUID-72EFCAB1-0B10-4007-A44C-09D38CD960D3.html

Take a snapshot of all VMware vSphere management VMs

Take a snapshot of VMware vSphere management VMs (vCSA and PSC) and Windows-based vCenter, database, and VM (If applicable).

To take a snapshot of all VMware vSphere management VMs. See the following applicable VMware guide:

For vSphere 6.0, see https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.hostclient.doc/GUID-878C36BA-6922-4269-8803-7FC419B947B7.html.

For vSphere 6.5, see https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-9720B104-9875-4C2C-A878-F1C351A4F3D8.html.

Upgrade components to the minimum required RCM versions

Upgrade all Converged System components, except the VMware components, to the required versions in the Converged System Release 6.7 RCM to which you are upgrading.

See the respective Software and Firmware Upgrade Guides for your Converged System for information about the process and order of upgrading these components.

Prepare for the VMware vCenter Server upgrade

To prepare for the VMware vCenter Server upgrade, address the customer-specific configuration requirements.

Review the following sections in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-671-upgrade-guide.pdf.

- System Requirements in the section *New vCenter Server Appliance and Platform Services Controller Appliance*
- System Requirements in *Migrating vCenter Server Deployments to vCenter Server Appliance Deployments*

Estimate upgrade time

Review the following considerations to ensure that you provide adequate scheduled maintenance windows to complete the upgrade.

Use the following table to calculate the time to upgrade the software and firmware on each component. If the Converged System that you are upgrading does not have a specific component in the table, skip that component.

- For cluster configurations, include both the primary and the subordinate components in the calculated time for the component.
- Plan your upgrade maintenance windows according to your environment. Do not upgrade all hosts at the same time. Retain an adequate number of hosts in a connected state to reduce impact to production traffic.
- For each upgrade task, record the total estimated upgrade time in the *Your Calculated Time* column of the following table.

ⓘ **NOTE:** The estimates do not include the time for preparation, configuration, backup, and download. Estimated times are may differ depending on applications running on your Converged System.

Order	Component	Minimum upgrade time (minutes)	Restart Required	Your Calculated Time
1	VMware vCenter Server Appliance with external PSC	60	Yes	
2	VMware vCenter for Windows Migrate or vCSA upgrade	60	Yes	
3	VMware ESXi hosts	35 per host	Yes	

Order	Component	Minimum upgrade time (minutes)	Restart Required	Your Calculated Time
4	Virtual Machines hardware version and VMware Tools	10	Yes	

The following table provides an estimated time based on the size of the database and the migration:

Database size	40 GB	75 GB	150 GB	250 GB
Migrating inventory and configuration data only (7 GB database)	30 minutes	30 minutes	30 minutes	30 minutes
Migrating inventory, configuration, event, and task data	1 hour, 4 minutes	1 hour, 49 minutes	3 hours, 19 minutes	5 hours, 48 minutes
Migrating all data (including performance and other historical data)	1 hour, 40 minutes	3 hours, 8 minutes	6 hours, 22 minutes	10 hours, 45 minutes

Pre-upgrade considerations for Enhanced Link Mode

Consider the following before starting the Enhanced Link Mode (ELM) upgrade.

- Upgrading a VxBlock System in a VMware vSphere 6.0 or 6.5 ELM configuration requires a corresponding upgrade for any other VxBlock System joined to the same VMware vSphere SSO domain.
- Create a backup of all PSCs configured in the ELM. Create simultaneous backups of all PSCs and VMware vCenter Servers participating in the ELM ring topology.
- Inventory and document all PSCs and VMware vCenter Servers participating in the same SSO domain before upgrade.
- Configure NTP for all PSCs.
- Verify the current status of the PSC by logging into the web interface for each PSC `https://<FQDN_PSC>:5480`. Use the username `root` and the Dell EMC standard password unless otherwise noted.
  1. Navigate to the **Summary** screen. Verify the following:
     - The build version is correct.
     - The **Overall Health** status is **Good**.
     - The SSO Domain Status is **RUNNING**.
  2. If the status does not meet the conditions, do not proceed with the upgrade until the PCSs meet these conditions.
  3. Enable SSH access to the PSC.
     (i) **NOTE:** Make sure the partner server is 0 changes behind. If any of the PSCs are not synchronized with each other, do not proceed with the upgrade until all PSCs display **Partner is 0 changes behind**. See *Verifying PSC and PSC Partner Status* in the Administration Guide for your Converged System.

Part III - Upgrade to VMware vSphere

Upgrade recommendations

Some Converged System components are optional or specific to a customer environment. If the Converged System that you are upgrading does not have a specific component, skip that component. When the component is in a cluster configuration, upgrade the subordinate component before you upgrade the primary component.

Upgrade the AMP before upgrading the Converged System. You can upgrade the AMP in a separate maintenance window.

Make sure your Converged System is upgraded according to the RCM. Refer to *Upgrade Converged System components to the minimum versions*.

ⓘ **NOTE:** VMware vSphere 6.7 is the last VMware vSphere release to support the deployment of external VMware PSCs. Updates to VMware vSphere 6.x support Enhanced Linked Mode in embedded VMware PSCs, making external VMware PSCs no longer necessary. Upgrading to VMware vSphere 6.7 update 1 or VMware vSphere 6.5 update 2d enables you to migrate external VMware PSCs to embedded VMware PSCs. For more information about changing to embedded VMware PSCs from external VMware PSCs, consult with your Dell Technologies Sales Engineer.

Upgrade the AMP components

The topics in this section explain how to upgrade the AMP components.

VMware vCenter Server components upgrade considerations

Scenarios for upgrading VMware vCenter Server components.

ⓘ **NOTE:** The following upgrade/migrations are not supported:

- VMware vCenter Server 6.0 on Windows/vCSA with Embedded SSO
- VMware vCenter Server 6.0 on Windows to VMware vCenter Server 6.7 on Windows

As a part of the upgrade, these components are converted as noted in the **Destination VMware vSphere 6.7** column. The following table describes supported scenarios:

Scenario	Source VMware vSphere 6.0 or 6.5	Destination VMware vSphere 6.7
vCSA with External PSC	VMware vCenter Server Appliance 6.0 - External PSC - Embedded database - External VUM	VMware vCenter Server Appliance - External PSC - Embedded DB-Postgres - Internal VUM
vCenter for Windows with External PSC	VMware vCenter for Windows 6.0 - External PSC - External database - External VUM	VMware vCenter Server Appliance - External PSC - Embedded DB-Postgres - Internal VUM
vCSA with external PSC	VMware vCenter Server Appliance 6.5 - External PSC - External DB-Postgres - Internal VUM	VMware vCenter Server Appliance - External PSC - External DB-Postgres - Internal VUM

> **NOTE:**
> 1. If upgrading a system with multiple VMware vCenter Servers in the same domain, complete the steps on each VMware vCenter Server. Repeat each procedure on each VMware vCenter Server – one at a time.
> 2. If upgrading the AMP-VX components, first upgrade the management PSC/VCSA and then all production PSCs/VCSAs sequentially.

> **NOTE:** If deploying, upgrading, migrating, or restoring to VMware vCenter Server Appliance 6.7
> release fails, see the following: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/
> GUID-30C9DC56-11AC-4C7E-9D67-1BEEDD53BE4E.html

Upgrade sequence for VMware vSphere on AMP-VX

For AMP-VX, upgrade the VMware vSphere components in the following sequence:
1. AMP-VX Management PSCs
2. AMP-VX Management vCenter Server
3. AMP-VX ESXi host
4. AMP-VX vSAN cluster
5. Production PSC
6. Production vCenter Server
7. Production ESXi

> **NOTE:** Before upgrading VxBlock 1000, upgrade all AMP components first.

Upgrade the external Platform Services Controller (PSC)

Upgrade the external PSC from version 6.0 or 6.5 to version 6.7 before upgrading VMware vCenter Server.

About this task

Upgrade the secondary PSC before upgrading the primary PSC.

> **NOTE:** If the environment has VMware NSX, repoint the NSX Manager to the primary PSC after the successful upgrade.

Steps

1. Log in to the PSC GUI **https://PSC-FQDN:5480** using the root password. Change the root password to a temporary password. See the following KB article: https://kb.vmware.com/s/article/2150683.

   > **NOTE:** A long-term root password is set during the appliance deployment GUI.

2. Download the vCSA installer ISO file and mount it to a network VM or physical server from which you want to perform the image upgrade: VMware-VCSA-all-version_number-build_number.iso
3. Confirm that the **md5sum** is correct.
4. Mount or extract the ISO image to the client machine from which you want to upgrade the appliance.
5. In the vCSA installation directory found in Windows explorer, go to the **vcsa-ui-installer\win32** folder, click **installer.exe**.
6. Click **Upgrade** to proceed.
7. On the **Introduction** page, click **Next**.
8. Accept the license agreement. At the **EULA** page, click **Next**.
9. Upgrade the existing PSC appliance using the information in the following table:

Connect to source appliance	Selection
Appliance FQDN or IP address	FQDN of secondary PSC
Appliance HTTPS port	443 (default)
Appliance (operating system) root password	Root password

Connect to source appliance	Selection
VMware vCenter Server name	vCenter FQDN
HTTPS port	443 (default)
User name	administrator@vsphere.local
Password	SSO password
SSL Cert	Accept SSL Cert warning

Appliance deployment target	Selection
VMware ESXi host or VMware vCenter Server name	vCenter FQDN
HTTPS port	443 (default)
VMware vCenter User name	administrator@vsphere.local
SSO Password	SSO password
SSL Cert	Accept SSL Cert warning

10. Select **Virtual DataCenter**. At the select folder page, click **Next**.
11. In the AMP cluster, select an ESXi server. At the **Select Compute Resource** page, click **Next**. Use the information in the following tables:

Setup Target Appliance VM	Selection
VM Name	New temporary secondary PSC VM name
root password	Root password - confirm the password

Select Datastore	Selection
Datastore	PSC Storage location
Enable Thin Disk mode	Thin Disk Mode

Configure network settings	Selection
Network	ESXi MGMT VLAN
IP Version	IPv4
IP Assignment	Static
Temporary IP Address	Temporary IP address on the ESX MGMT subnet
Subnet Mask or Prefix Length	Subnet mask
Default Gateway	Default GW on the ESX MGMT subnet
DNS Server	DNS server IP address

12. At the **Ready to complete stage 1** page, verify the configuration and click **Finish**.
13. After stage 1 has finished, click **Continue**.
14. On the **Introduction** page, click **Next**.
15. On the **connect to source PSC** page, enter the SSO password, then click **Next**.
16. Deselect **CEIP**, then click **Next**.
17. On the **Ready to Complete** page, select **I have backed up the source PSC**, then click **Finish**.
18. When prompted with the **Shutdown** warning dialog box, click **OK** to initiate upgrade.
19. Acknowledge the TLS version changes message. Click **Close**. Verify that you can log in to the VMware vCenter Server.
20. Repeat the procedure for each peer PSC, one at a time.

Pointing NSX Manager to secondary PSC

For systems with NSX follow this task to point the NSX Manager to the upgraded secondary PSC.

Steps

1. Open the browser and enter FQDN or the IP address of each NSX Manager.
2. Login using admin credentials.
3. Click **Manage vCenter Registration**.
4. Click **edit** under **Lookup Service URL**.
5. Type FQDN and SSO admin credentials of the upgraded secondary PSC. Click **OK**.
6. Click **Yes** to **Accept Trust Certificate** to complete the registration.
7. Follow the instructions to repoint the vCenter to the upgraded primary PSC in the same domain provided in VMware KB:
   https://kb.vmware.com/s/article/2113917

Pointing NSX Manager to the primary PSC

For systems with NSX, use this procedure to repoint NSX Manager to the upgraded primary PSC.

Steps

1. Open a browser and enter the FQDN or IP address of each NSX Manager.
2. Log in using admin credentials.
3. Click **Manage vCenter Registration**.
4. Click **edit** under **Lookup Service URL**.
5. Enter the FQDN and SSO admin credentials of the upgraded PSC and click **OK**.
6. To complete the registration, click **Yes** when prompted to **Accept Trust Certificate**.

Upgrading the VMware NSX Environment

VMware NSX 6.4.x or higher is required before continuing the VMware vSphere or vCenter upgrade to version 6.5.

If VMware NSX 6.2.x is in your environment, see the *Dell EMC VxBlock Systems Upgrade Guide from VMware NSX 6.2.x to VMware NSX 6.4.x.*

Upgrade the VMware vCenter Server Appliance

Upgrade the vCSA 6.0 to vCSA 6.7

Upgrade the vCSA 6.0 with an external VUM to vCSA 6.7 with an integrated VUM.

About this task

Before the upgrade, you must run the migration assistant tool on the VUM server to collect the required data and integrate with vCSA 6.7.

Perform this upgrade only if you can resolve vCSA FQDN using DNS. Make sure all the prerequisites of DNS/FQDN and NTP are configured according to VMware guidelines.

The VMware vCenter Server Appliance upgrade process runs in three stages:
* Stage1 - Run the migrations assistant tool on the VUM server to collect the required data and integrate with vCSA 6.7.
* Stage 2 - Launch the upgrade to deploy the vCSA 6.7.
* Stage 3 - Point to the existing PSC and migrate the data to newly deployed vCSA.

Steps

1. Log in to the vCSA GUI (https://VCSA-FQDN:5480) using the root password and change the root password to a temporary password. Set the root password to a longer term password during the appliance deployment GUI.

2. Verify that all prerequisites are performed. See the *Prerequisites for Upgrading the vCenter Server Appliance or Platform Services Controller Appliance* topic in the *vSphere vCenter Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-671-upgrade-guide.pdf.

3. Identify the IP address on same subnet as the existing vCSA VM for temporary assignment during the upgrade process.

4. Mount the vCSA 6.7 Installer ISO on the VUM and copy the **Migration Assistant** folder on the ISO to the VUM Windows machine. Run `VMware-Migration-Assistant.exe` from the local copy. Enter the SSO password and follow the instructions for a VCSA upgrade.

5. Perform the tasks that are outlined in the *GUI Upgrade of the vCenter Server Appliance and Platform Services Controller Appliance* in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-671-upgrade-guide.pdf

   (i) **NOTE:** If the configuration requires a VMware vCenter ESXi host with more than the following, verify that the appliance deploy size is large or extra large:
   - 512 LUNs
   - 2,048 paths to the vCenter Server Appliance

6. Repeat the VMware vCenter upgrade/migration procedure for the other VMware vCenter Servers in the same domain. Repeat each procedure on each VMware vCenter Server, one at a time.

7. After the vCSA upgrade is complete, log in to the VMware vSphere HTML5 Client to validate that the vCSA is operational. For example: `https://<FQDN or IP>/ui`

Upgrade the vCSA 6.5 to vCSA 6.7

Upgrade the vCSA 6.5 to vCSA 6.7 with integrated VUM.

About this task

Perform this upgrade only if you can resolve vCSA FQDN using DNS. Make sure all the prerequisites of DNS/FQDN, and NTP are configured according to VMware guidelines.

The VMware vCenter Server Appliance upgrade process runs in two stages:
1. Stage 1 - OVA deployment
2. Stage 2 - Appliance setup

Prerequisites

1. Verify that all prerequisites are performed as indicated in one of the following topics in the *vSphere vCenter Server Upgrade* documentation:
   - *Prerequisites for Upgrading the vCenter Server Appliance* or
   - *Platform Services Controller Appliance*
   https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-671-upgrade-guide.pdf

2. Identify the IP address on same subnet as the existing vCSA VM for temporary assignment during the upgrade process.

3. Log in to the vCSA GUI **https://VCSA-FQDN:5480** using the root password and change the root password to a temporary password. Set the root password to a longer term password during the appliance deployment GUI.

Steps

1. Download the vCSA installer ISO file and mount it to a network VM or physical server from which you want to perform the image upgrade: **VMware-VCSA-all-version_number-build_number.iso**

2. Confirm that the **md5sum** is correct.

3. Mount or extract the ISO image to the Element Manager VM.

4. In the vCSA installation directory found in Windows explorer, go to the **vcsa-ui-installer\win32** folder, click **installer.exe**.

5. Click **Upgrade**.

6. On the **Introduction** page, click **Next**.

7. Accept the license agreement. At the **EULA** page, click **Next**.

8. Connect to the vCSA that you want to upgrade.

a. Enter the information about the source vCSA that you want to upgrade and click **Connect to Source**.
b. Enter the information about the vCenter Single Sign-On administrator and root user.
c. Enter the information about the source ESXi host or vCenter Server instance with the vCSA that you want to upgrade and click **Next**.

Use the information in the following table:

Connect to source appliance	Selection
Appliance FQDN or IP address	FQDN of vCenter Server
Appliance HTTPS port	443 (default)
SSO User name	administrator@vsphere.local
SSO Password	SSO Password
Appliance (operating system) root password	Root password
ESXi host or VMware vCenter Server name	vCenter FQDN
HTTPS port	443 (default)
User name	administrator@vsphere.local
Password	SSO password

9. Verify that the certificate warning displays the SHA1 thumbprints of the SSL certificates that are installed on the source appliance and source server. Click **Yes** to accept the certificate thumbprints.
10. Connect to the target server on which you want to deploy the new vCSA using the information in the following table:

Appliance deployment target	Selection
VMware ESXi host or VMware vCenter Server name	FQDN or IP address of the ESXi host
HTTPS port	443 (default)
ESXi host User name	root
SSO Password	root Password
SSL Cert	Accept SSL Cert warning

(i) **NOTE:** The target server cannot be the vCSA that you want to upgrade. In such cases, use an ESXi host as a target server.

11. Select **Virtual Datacenter**. At the select folder page, click **Next**.
12. On the **Setup target appliance VM** page, enter a name for the new vCSA, set the password for the root user, and click **Next**.

(i) **NOTE:** The root password of the old appliance is not transferred to the new upgraded appliance.

13. For your VMware vSphere inventory, select the **deployment size** for the new vCSA.
14. Select the storage size for the new vCSA, and click **Next**.

(i) **NOTE:** If the configuration requires a VMware vCenter ESXi host with the following characteristics, set the appliance deploy size to large or extra large:

- More than 512 LUNs
- More than 2,048 paths to the vCSA

15. From the list of available datastores, select the location to store the VM configuration files and virtual drives.
16. Enable thin provisioning by selecting **Enable Thin Disk Mode**, and then click **Next**.
17. Configure the temporary network for communication between the vCSA that you want to upgrade and the new vCSA and click **Next**.

Configure network settings	Selection
Network	ESXi MGMT VLAN
IP Version	IPv4
IP Assignment	Static
Temporary IP Address	Temporary IP address on the ESX MGMT subnet
Subnet Mask or Prefix Length	Subnet mask
Default Gateway	Default GW on the ESX MGMT subnet
DNS Server	DNS server IP address

(i) **NOTE:** For AMP-VX ESXI MGMT, the VLAN name is **amx_esx_mgmt** otherwise **vcesys_esx_mgmt**.

18. On the **Ready to complete stage 1** page, review the deployment settings for the new vCSA and then click **Finish** to start the OVA deployment process.
19. When the OVA deployment process finishes, click **Continue** to proceed with stage 2 of the upgrade process. Stage 2 transfers the data from the old appliance and starts the services of the new appliance.
20. Review the introduction to stage 2 of the upgrade process, and then click **Next**.
21. Wait for the preupgrade check to finish.
22. On the **Select Upgrade data** page, choose the data that you want to copy from the old appliance to the upgraded appliance, and click **Next**.
23. On **Ready to Complete** screen check **I have backed up the source PSC**. Click **Finish** to initiate the upgrade.
24. Click **OK** to acknowledge the shutdown warning.
25. After the upgrade is complete, log in to the vCenter Server to verify that the upgrade was successful.
26. Repeat the VMware vCenter upgrade procedure for other VMware vCenter Servers in the same domain. Repeat each procedure on each VMware vCenter Server – one at a time.
27. After the vCSA upgrade is complete, log in to the VMware vSphere HTML5 Client to validate that the vCSA is operational. For example: `https://<vCenter FQDN or ip>/ui`

Migrate from the VMware vCenter 6.0 Server running on Windows to vCSA 6.7

Perform this procedure to upgrade VMware vCenter Server running on Microsoft Windows.

About this task

Use this procedure to migrate the VMware vCenter Server with external VUM and External Microsoft SQL database and validate the installation.

Prerequisites

Before you migrate the Windows-based VMware vCenter, upgrade PSCs as described in *Upgrading the Platform Services Controller Appliance*. Follow the *Migrating vCenter Server for Windows to vCenter Server Appliance* in the chapter 5 of the *VMware vCenter Server Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-vcenter-server-671-upgrade-guide.pdf

Steps

1. Verify that the VMware vCenter Server configuration and database are backed up.
2. If you get an error stating `add process level token`, do the following:
   a. Access the Windows vCenter Server as a vcenterSA user using RDP Under **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **User Rights Assignment**.
   b. Set the **Process Level Token** for the vumSA user.
   c. Double-click **Replace a process level token**, and then add the **VMNAME\vumSA** user.
   d. Click **OK**.

3. Mount the vCSA 6.7 Installer ISO on the VUM. Log in to the VUM Server through RDP as a vumSA user. Copy the **Migration Assistant** folder on the VUM Windows machine and run **VMWare-Migration-Assistant.exe**.

   a. Copy the **Migration Assistant** folder on the VUM Windows machine.

   b. In the **Migration Assistant** folder, run **VMWare-Migration-Assistant.exe**.

   c. Enter the SSO password in the dialog box. Running the prechecks and preparing the migration takes several minutes. Run the **Migration Assistant** on the vCenter server.

4. Mount the vCSA 6.7 Installer ISO on the VMware vCenter 6.7. Log in to VMware vCenter Server through RDP as a vCenterSA user.

   a. Copy the **Migration Assistant** folder on the desktop.

   b. In the **Migration Assistant** folder, run the **VMWare-Migration-Assistant.exe**.

   c. Enter the SSO password and the vCenterSA password when prompted with the dialog box.

   d. Make a note of the recommended deployment size to use in a subsequent step in this task.

5. Make a note of the recommended deployment size to use in a subsequent step in this task.

6. Mount the vCSA 6.7 Installer ISO on the Element Manager machine. Connect to the Element Manager using RDP and run the DVD: **/vcsa-ui-installer/win32/installer.exe**.

7. Select **Migrate** in the Installer.

   a. Click **Next** on the introduction page.

   b. Accept EULA and click **Next**.

   c. Enter the VMware vCenter Server FQDN. Alternatively, you can enter the IP address and leave the Migration Assistant port to the default (for example, 9123). Enter the SSO credentials and click **Next**.

   d. Click **YES** on SSL certificate warning.

   e. From the **Appliance Deployment Target** page, enter the VMware vCenter FQDN with SSO login credentials.

   f. Accept the Certificate Warning by clicking **YES**.

   g. On the **Select Folder** page, select the Virtual Datacenter where the target ESXi (AMP) is present, and then click **Next**.

   h. On the **Select folder** page, expand the AMP cluster and select the ESXi cluster and then click **Next**.

   i. On the **Select Compute resource**, select the ESXi host and then click **Next**.

   j. On the **Setup Target appliance VM** page, enter a VM name for the VMware vCenter Server Appliance and enter the root password, and then click **Next**.

   k. Select the following:

      i. Select the deployment size as per the client size and click **Next** depending on the existing implementation (usually **Medium**). If the configuration exceeds 400 hosts and 4000 VM limits, then select **Large**.

      ii. Select the storage size as default and then click **Next**.

Deployment type	Default storage size	Large storage size	X-Large storage size
Tiny environment (up to 10 hosts or 100 virtual machines)	300 GB	825 GB	1700 GB
Small environment (up to 100 hosts or 1,000 virtual machines)	340 GB	870 GB	1750 GB
Medium environment (up to 400 hosts or 4,000 virtual machine)	525 GB	1025 GB	1905 GB
Large environment (up to 1,000 hosts or 10,000 virtual machines)	740 GB	1090 GB	1970 GB
X-Large environment (up to 2,000 hosts or 35,000 virtual machines)	1180 GB	1230 GB	2110 GB

   l. Select the target datastore for VMware vCenter Server and check **Enable Thin Disk mode** and click **Next**.

   m. On **Configure network settings** page, keep the following values:

Wizard setting	Selection
Network	vcesys_esx_mgmt

Wizard setting	Selection
IP Version	IPV4
IP Assignment	Static
Temporary IP Address	Temporary IP address
Subnet Mask or Prefix Length	Subnet mask
Default Gateway	Default GW
DNS Server	Enter the DNS server IP addresses, separating them with commas.

    n. Verify the given details and click **Finish**.

8. After the deployment has been completed, on the **Upgrade - Stage 1** page, click **Continue**.

9. Click **Next** on the **Introduction** page.

10. Close the warning.

11. If the VMware vCenter Server is a member of an Active Directory, you are prompted to enter an AD user. The user must have permissions to add a host to the AD domain and the format must be: `user@ADdomainName`

12. On the **Select Migration data**, select the option that matches the system requirements and click **Next**.

13. Review the settings, check the box for backup, and click **Finish**.

14. Click **OK** to continue.

This wizard continues to migrate data. When migration is done, the wizard powers off the old VMware vCenter Server and starts the vCSA 6.7 with an internal vPostgress database and internal VUM.

> (i) **NOTE:** During the data migration, there is a service disruption to the VMware vCenter Server logins. However, all VMware vCenter operations are not affected.

> (i) **NOTE:** Repeat the VMware vCenter upgrade/migration procedure for other VMware vCenter Servers in the same domain. Repeat each procedure on each VMware vCenter Server, one at a time.

Upgrade VMware ESXi hosts

This section defines the workflow to upgrade AMP hosts and compute hosts for VMware vSphere.

Upgrade AMP ESXi hosts

Update the AMP VMware vSphere ESXi hosts.

About this task

Before upgrading the AMP Management VMware vSphere ESXi hosts, consider the following:
- VMware provides several ways to upgrade VMware vSphere ESXi hosts. Use VUM and a custom VMware vSphere AMP-specific ESXi ISO image to upgrade the hosts in the Converged System.
- Verify that PowerPath modules are not present. If they exist, remove them before proceeding with the upgrade.
- (i) **NOTE:** The following statement does not apply to AMP-2V because it uses production servers:

  If upgrading a non-HA AMP with a single Cisco UCS C-Series Server, shut down all the AMP VMs and upgrade the Cisco UCS C-Series Server interactively. Use the AMP-specific ESXi ISO image obtained in preupgrade tasks. See the *Upgrade Hosts Interactively* section of the *VMware ESXi Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.esxi.upgrade.doc/GUID-77D42D81-F47E-4FE9-B4B2-B15AB16C9C1A.html
- To ensure that remediation is successful, temporarily disable the following features in the Remediation Cluster Settings:
  - Distributed Power Management (DPM)
  - HA admission control
  - Fault Tolerance
- If the VUM displays a warning about incompatibility, confirm that the NTP client is configured. If it is not, for each host configure NTP, reboot, and rescan against the AMP-specific VMware vSphere ESXi ISO upgrade image. See the *Configuring the NTP client* section in the applicable Converged System Administration Guide.

- If any VUM upgrade warnings cannot be resolved, you may need to upgrade the hosts interactively. See the *Upgrade Hosts Interactively* section of the *VMware ESXi Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.esxi.upgrade.doc/GUID-77D42D81-F47E-4FE9-B4B2-B15AB16C9C1A.html
- If upgrading an HA AMP, place one of the Cisco UCS C-Series Servers in maintenance mode and upgrade the VMware vSphere ESXi host:
  - Ensure that you have access to the AMP-specific VMware vSphere ESXi ISO image obtained in the preupgrade tasks.
  - Use the VUM to complete the upgrade to VMware vSphere 6.7. See the *Using the Remediate Hosts against an Upgrade Baseline* section of the *Installing and Administering VMware vSphere Update Manager* documentation.

Prerequisites

Perform the following steps to upgrade VMware vSphere ESXi hosts with the following AMPs: AMP-2P, AMP-2S, AMP-3S, and AMP-VX.

(i) **NOTE:** For AMP-2V, do not perform this procedure. Continue to the topic *Upgrading Compute VMware vSphere ESXi hosts*.

Alternatively, you can upgrade hosts interactively. See the *Upgrade Hosts Interactively* section of the *VMware ESXi Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/%20com.vmware.esxi.upgrade.doc/GUID-77D42D81-F47E-4FE9-B4B2-B15AB16C9C1A.html

Steps

1. Log in to the VMware vCenter Server using HTML5 client by entering `https://<fqdn-vCenter` or `IP>/ui` in browser.
2. Record all VMware vSphere ESXi host and datastore locations of all management AMP VMs. You may need this information at the end of the procedure.
3. Under the **Menu** drop-down, select **Update Manager**.
4. On the **vSphere Update Manager** page, click **ESXi images** tab on the right and then click **Import** to upload the AMP ESXi Image.
5. On the **Import ESXi Image** window, locate the AMP ESXi 6.7 ISO and then click **Import**.

   (i) **NOTE:** For AMP-VX, use the custom Dell PowerEdge AMP-VX ESXi image only.

6. On the **Baselines** tab, click **NEW** > **New Baseline**.
7. On the **Baseline Definition** page, under **Name** enter `AMP Upgrade` and `AMP Baseline` for the new baseline, and then click **Upgrade baseline** > **Next**.
8. On the **Select Image** page, select the AMP ESXi 6.7 ISO, and then click **Next**.
9. On the **Summary** page, validate the details, and then click **FINISH**.
10. To attach the newly created baseline, under **Hosts and Clusters** > **Maintenance** select the AMP cluster, and then go to **Updates** > **Host Updates**.
11. Click **Attach** and then select **AMP Upgrade** baseline.
12. On the host selected for the upgrade, perform a vMotion on AMP VMs to the other hosts in AMP cluster.
13. Place the selected AMP host in maintenance mode.

    (i) **NOTE:** For AMP-VX ESXi hosts, select the **ENSURE ACCESSIBLITY for vSAN data migration** option when entering maintenance mode.

14. Select AMP cluster, on the **Updates** tab, select **Host Updates**.
15. Select the **AMP Upgrade** baseline, and then click **Remediate**.
16. Accept the VMware EULA and click **OK**.
17. To start the upgrade, select the AMP host that is manually under maintenance and click **REMEDIATE**.
18. Verify that the VMware vSphere ESXi host reconnects to VMware vCenter successfully, and then exit maintenance mode.
19. Repeat Steps 12–18 for rest of the AMP hosts.

Upgrade the Compute VMware vSphere ESXi hosts

Guidelines and instructions for upgrading the compute VMware vSphere ESXi hosts.

About this task

These instructions explain how to load ESXi ISO images are loaded into Update Manager, create baselines, and execute ESXi upgrades on compute hosts.

Prerequisites

Before upgrading the Converged System compute VMware vSphere ESXi hosts, consider the following:

- Although VMware provides several ways to upgrade vSphere ESXi hosts, you must use VMware vSphere Update Manager and custom VMware vSphere ESXi ISO image to upgrade the compute hosts in the Converged System.
- Do not upgrade all of the hosts at the same time. Keep enough hosts online to reduce impact to production traffic.
- If you have VMware Distributed Power Management (DPM), HA admission control, or Fault Tolerance enabled, temporarily disable these features in the Remediation Cluster Settings to make sure that the remediation is successful.
- If the VMware vSphere Update Manager displays a warning about incompatibility, confirm the NTP client is configured and clocks are synchronized. If the NTP client is not configured and the clocks are not synchronized, for each host configure NTP, reboot, and rescan against the custom ISO upgrade image. Refer to Configuring the NTP client section in the Converged System Administration Guide for your Converged System.

  Use a VMware vSphere 6.7 boot LUN size of 15 GB to facilitate the ESXi scratch partition.

- If the VMware vSphere Update Manager displays upgrade warnings that cannot be resolved, you may need to upgrade the hosts interactively. Refer to the Upgrade or Migrate Hosts Interactively section of the VMware vSphere Upgrade documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-671-upgrade-guide.pdf

Use a VMware vSphere 6.7 boot LUN size is a minimum of 15 GB to facilitate the ESXi core dumps. Consult your Converged System Administration Guide for steps to expand LUNs.

To increase the boot LUN size, connect to the storage management and select the host to which you want to make changes. Select the boot LUN and edit the size.

Save the changes and reboot the host to reflect the new boot LUN size.

After the host reboots, extend the size of hostname_localstorage.

Steps

1. Log in to VMware vCenter Server using an HTML5 client by entering **`https://<FQDN-vCenter>/ui`** in the browser.
2. Record all VMware vSphere ESXi host and datastore locations of all production VMs.
3. Under the **Menu** dropdown, select **Update Manager**.
4. On the **Update Manager** page, click the **ESXi images** tab on the right, and then click **Import** to upload Cisco UCS B- or C-series Server Compute ESXi images.
5. On **Import ESXi Image** window, locate the Compute ESXi 6.7 ISO for Cisco UCS B-Series or C-Series and click **Import**.
6. Select the **Baselines** tab and click **NEW** > **New Baseline**.
7. On the **Baseline Definition** page, update the following information:
   a. Under **Name** enter **`Compute Upgrade <RCM version>`**.
   b. Under **Description** enter **`Compute Baseline`** for the new baseline.
   c. For **Content**, select **Upgrade**.
   d. Click **Next**.
8. On the **Select Image** page, select the compute ESXi 6.7 image that was uploaded earlier, and then click **Next**.
9. On the **Summary** page, validate the details, and then click **FINISH**.
10. To attach the newly created baseline, under select the compute cluster, and then select **Hosts and Clusters** > **Updates** > **Host Updates**.
11. Click **Attach** and then select **Compute Upgrade** baseline. Click **Attach**.
12. On the compute hosts selected for the upgrade, perform vMotion on the production VMs to the other hosts in compute cluster.
13. Place the selected compute host in maintenance mode.
14. Select the compute cluster on the **Updates** tab, select **Host Updates**.
15. Select the **Compute Upgrade** baseline, and then click **Remediate**.

16. Accept the VMware EULA and click **OK**.
17. To start the upgrade, select the Compute host that is manually under maintenance and click **REMEDIATE**.
18. Verify the VMware vSphere ESXi host reconnects to VMware vCenter successfully and then exit maintenance mode.
19. Repeat Steps 12–18 for the rest of the compute hosts in the cluster.
20. Repeat Steps 12–19 for the rest of the compute clusters.
21. Enable the VMware Distributed Power Management (DPM), HA admission control, or Fault Tolerance that was temporarily disabled before the upgrade.

Verifying ESXi VIBs in the NSX environment

Complete this task to upgrade ESXi VIBs in the NSX environment.

Steps

1. Verify the ESXi of the compute and edge cluster.
2. Upgrade the NSX VIBs.

   a. Navigate to **Networking & Security** > **Installation and Upgrade** > **Host Preparation**
   b. Select Edge cluster and click **Actions > Resolve** to trigger the NSX VIB upgrade.
   c. Select each compute cluster and click **Actions > Resolve** to trigger the NSX VIB upgrades.

   ⓘ **NOTE:** If you are upgrading from ESXi 6.0 and the cluster has DRS enabled, DRS will attempt to put the host into maintenance mode in a controlled fashion that allows the VMs to continue running. If DRS fails for any reason, the resolve action halts. In this case, you may need to move the VMs manually and then retry the Resolve action or put the host into maintenance mode manually.

   d. For Cross-vCenter, select each secondary NSX manager and perform step c for all Compute clusters.

Upgrade the VMware vSphere Distributed Switch (VDS)

Upgrade the VMware vSphere Distributed Switch.

Steps

1. Connect to the VMware vCenter Server using the VMware vSphere HTML5 client by entering `https://<fqdn-vCenter>/ui` in browser.
2. Follow the *Upgrade a vSphere Distributed Switch to a Later Version* procedure of the *Setting Up Networking with vSphere Distributed Switches* section within the *VMware vSphere Networking* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.networking.doc/GUID-330A0689-574A-4589-9462-14CA03F3F2F4.html
3. Repeat step 1 and 2 for each VDS configured.

Upgrade the vSAN disk format on AMP-VX cluster

About this task

Upgrade the AMP-VX cluster up in the following sequence:
1. VMware vCenter Server.
2. VMware ESXi hosts.
3. vSAN disk format.

⚠ **CAUTION: Failure to follow the sequence of upgrade tasks leads to data loss and cluster failure.**

Prerequisites

● Ensure you have a full backup of all data stored on the vSAN before upgrading.

- The disk groups are upgraded one at a time. For each disk group upgrade, all data from each device is evacuated and the disk group is removed from the vSAN cluster. The disk group is then added back to vSAN with the new on-disk format.
- Ensure that enough free space is available. The space available must equal the logical consumed capacity of the largest disk group. You need a separate disk group with the available capacity from the one you are migrating.
- ⚠ **WARNING: While the upgrade is in progress, do not remove or disconnect any host, and do not place a host in maintenance mode. When any member host of a vSAN cluster enters maintenance mode, the member host no longer contributes capacity to the cluster. The cluster capacity is reduced and the cluster upgrade might fail.**
- Verify that the disks are in a healthy state. Navigate to the **Disk Management** page to verify the object status.

ⓘ **NOTE:** Once you upgrade the on-disk format, you cannot roll back software on the hosts or add certain older hosts to the cluster.

Steps

1. Navigate to the vSAN cluster.
2. Select the **Configure** tab.
3. Under **vSAN**, select **Disk Management**.
4. Click **Pre-check Upgrade**.

   ⓘ **NOTE:**

   The upgrade precheck analyzes the cluster to uncover any issues that might prevent a successful upgrade. Some of the items that are checked are host status, disk status, network status, and object status. Upgrade issues are displayed in the **Disk pre-check status** text box.

5. Click **Upgrade**.
6. On the **Upgrade** dialog box, ensure **Allow Reduced Redundancy** is cleared, and then Click **Yes** to perform the upgrade of the on-disk format.

Verify the vSAN cluster upgrade

Before you complete the upgrade of the vSAN cluster verify your Converged System is using latest version of VMware vSphere and vSAN.

Steps

1. Navigate to the vSAN cluster.
2. Select the **Configure** tab, verify that the vSAN is listed.

   ⓘ **NOTE:** You can also navigate to the ESXi host, and then select **Summary** > **Configuration**. Verify that the latest version of the ESXi host is in use.

Next steps

Update AMP Management VM VMware tools and virtual hardware version

Upgrade the VMware tools and virtual hardware version on the AMP Management VM.

Prerequisites

Perform this task during an application maintenance window, because it requires powering down and rebooting the VM.

ⓘ **NOTE:** Before upgrading, backup each of the VMs.

Steps

1. Upgrade the VMware tools for the Management VMs with Microsoft Windows Server OS (Element/Fabric Manager VMs).

   See the *Upgrade Virtual Machines and VMware Tools* procedure in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.update_manager.doc/GUID-0B9FF31B-3702-4BD2-B925-9DAC98051338.html

2. Upgrade the VM hardware to version 14 for the AMP Management VMs with Microsoft Windows Server OS (Element/Fabric Manager VMs).

   See the *Upgrade the Compatibility of a Virtual Machine Manually* procedure in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-60768C2F-72E1-42E0-8A17-CA76849F2950.html

   (i) **NOTE:** If upgrading the Element Manager, launch the vCenter HTML5 client from an off-platform browser.

3. Power on the VM

5

Part IV - Post-upgrade tasks

Install the VMware Enhanced Authentication plug-in

Install the VMware Enhanced Authentication plug-in.

About this task

See the instructions on installing the VMware Enhanced Authentication Plug in the
VMware document: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-E640124B-BB55-4D29-AADD-296E01CF88C8.html

Steps

1. Connect to the Element Manager using a Remote Desktop connection.
2. Log in using local administrator credentials.
3. Open the vSphere HTML5 client by entering `https://<fqdn-vCenter>/ui` in a browser.
4. At the bottom of the vSphere HTML5 Client login page, click **Download Enhanced Authentication Plug-in**.
5. If the browser blocks the installation by issuing certificate errors or running a pop-up blocker, follow the browser help instructions to resolve the problem.
6. Save the plug-in to your computer and run it.
7. Step through the installation wizard for both the VMware Enhanced Authentication plug-in service and the VMware Plug-in Service, which are run in succession.
8. When the installations are complete, restart your browser.

Re-register the Solution in VMware vCenter Server after upgrade or migration

After the certificate is regenerated during the upgrade or migration, re-register a previously registered solution and any third-party client plug-in packages with VMware vCenter Server.

About this task

VMware suggests re-registering VMware vCenter extensions after an upgrade. See the following *VMware vSphere Upgrade* documentation:

After Upgrading or Migrating vCenter Server > Re-register Plug-In Solution in vCenter Server After Upgrade or Migration

https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.upgrade.doc/GUID-E718867A-5131-4616-A030-C39BA3F94896.html

Consult the vendor documentation for any solution-based VMware vCenter extensions and client plug-ins for instructions to reregister after a VMware vCenter upgrade.

Verify VMware vCenter Server Appliance

Ensure that the VMware vCenter Server components are upgraded correctly.

About this task

If the VxBlock System does not have a specific component, skip that component and proceed with the next component.

Ensure that the VMware vCenter Server Appliance (vCSA) successfully upgraded for the AMP and Converged System by verifying the following:

- VMware vCSA instances are accessible.
- Inventory data is successfully migrated.
- VMware vCSA version comply with the supported versions in the VxBlock Systems Release Certification Matrix.
- All VMware licenses are applied and are not running in evaluation mode. The **Updates** tab in VMware vSphere vCenter Server is available on the HTML5 client.
- The updated versions comply with the supported versions in the VxBlock Systems Release Certification Matrix.
- VMware vSphere ESXi build numbers on the management environment and VMware ESXi hosts comply with the supported versions in the Converged Systems Release Certification Matrix.
- There is network connectivity to virtual machines, VLAN, and VSAN, if applicable.
- The time, date, and time zones are synchronized across all VMs and hosts.

Verify PSCs are configured in Enhanced Linked Mode (ELM)

Verify PSCs are configured in Enhanced Linked Mode (ELM).

Steps

1. Enable SSH and BASH on the PSCs.
   a. Open web browser to **https://<PSC_FQDN>:5480/ui** and log in with root credentials.
   b. Click **Access**, and then click **Edit** to enable SSH and BASH. Set the timeout to 20 minutes.
   c. Repeat steps 1a and 1b for each PSC.
2. Verify that the current partner servers exist for the upgraded PSC using the following steps:
   a. Use SSH to connect to the upgraded PSC.
   b. Launch the BASH shell by typing **shell**.
   c. Type **cd /usr/lib/vmware-vmdir/bin**
   d. Type **./vdcrepadmin -f showpartners -h localhost -u administrator**

   > (i) **NOTE:** When prompted, enter administrator SSO password.

   e. The command should display two partners for each PSC in a ring topology and single peer in a dual PSC deployment. The following is an example of the output:

   ```
   epscl:~#
   epscl:~# cd /usr/lib/vmware-wmdir/bin
   epsc1:/usr/lib/vmware-vmdir/bin # ./vdcrepadmin -f showpartner -h localhost -u
   administrator
   password:
   ldap://epsc2.pde.lab.vce.com
   ldap://epsc7.pde.lab.vce.com
   ```

3. Verify the current partner server status for the upgraded PSC using the following command:
   a. Type **/vdcrepadmin -f showpartnerstatus -h localhost -u administrator**
   b. This command shows a sequence number for both PSCs. Each PSC uses a unique change number and should be zero changes behind. The following is an example of the output:

   ```
   epsc1:/usr/lib/vmware-vmdir/bin # ./vdcrepadmin -f showpartnerstatus -h localhost
   -u administrator
   password:
   ```

```
Partner: espc2.pde.lab.vce.ocm
Host available: Yes
status available: Yes
My last change number:   12605
Partner is 0 changes behind.

Partner: epsc7.pde.lab.vce.com
Host available:  Yes
Status available: Yes
My last change number: 12605
Partner has seen my change number: 12605
Partner is 0 changes behind.
```

4. Repeat the preceding steps for all PSCs in the ELM topology.
5. Disable SSH and BASH after verifying the PSC partners and status.

> (i) **NOTE:** After the VMware vCenter Server upgrade, the higher version (upgraded) VMware vCenter Server that is configured in ELM can manage the lower version VMware vCenter Server. However, the lower version VMware vCenter Server cannot manage the upgraded higher version VMware vCenter Server in ELM.

Verify compliance with the RCM

Verify that the upgraded components match the versions that are listed in the RCM.

Confirm that the Converged System components match the versions of software, firmware, and hardware listed in the *Release Certification Matrix* for your Converged System.

See the appropriate *Release Notes* for information about installing necessary patches or updates.

Install VMware vCenter Server root certificates on the web browser

Verify that root certificates are installed. If not, follow the steps to install them.

About this task

Install the trusted root certificate authority (CA) certificates. Perform this procedure on Internet Explorer (IE) only. For browsers other than Internet Explorer, see the respective browser documentation.

Steps

1. Open web browser and go to **https://<vcsa_fqdn>**.
2. In the VMware vCenter **Getting Started** page, select **Download trusted root CA certificates** and save the file locally.
3. Unzip the downloaded files.
4. Go to the **win** folder inside the unzipped folder.
5. Right-click each `.crt` file and click **Open**.
6. In the dialog box, click **Install Certificate**.
7. Select **Local Machine** > **Next** > **Finish**.

Verify VMware ESXi advanced settings

Verify that the NFS settings are configured for optimal Converged System performance.

In VMware vSphere ESXi 6.7, the number of outstanding I/O requests with competing parameters is limited to the Max Queue Depth of a device. Depending on the storage array, the system may require a change to the Disk.SchedNumReqOutstanding (DSNRO) on ESXi.

See the *Configuring advanced settings* section of the *Administration Guide* for your Converged System.

The vStorage APIs for array integration (VAAI) primitives are enabled by default upon the initial installation of VMware vSphere ESXi. They should remain set to their current value (enabled or disabled) for all VMware ESXi hosts, except for the following conditions:

- If there is a specific customer or vendor reason for disabling primitives
- If there is a recall of a primitive based on outstanding issues in related software releases

Parameter name	XtremIO	Unity	VMAX or PowerMax
FC Adapter Policy IO Throttle Count	1024 MB (No action needed, value set in UCS)	256 MB (default)	256 MB (default)
fnic_max_qdepth	128 MB	32 MB (default)	32 MB (default)
Disk.SchedNumReqOutstanding	128 MB (vSphere 6.5)	32 MB (default)	32 MB (default)
Disk.SchedQuantum	64 MB	8 MB (default)	8 MB (default)
Disk.DiskMaxIOSize	4 MB	32 MB (default)	32 MB (default)
XCOPY	4 MB	16 MB	240 MB
vCenter Concurrent Clones	8 per X-Brick (up to 48 MB)		

ⓘ **NOTE:** Customers who upgrade and have existing VMAX claim rules can continue to use VMW_VAAIP_SYMM.

Create Cisco UCS adapter settings

Review and verify that the Ethernet Adapter policy and Virtual Machine Queue (VMQ) connection policies are configured in the Cisco UCS Manager using standard practices. Verify that the service profiles are updated. Create VMQ policies and apply them to the Ethernet adapters.

About this task

Verify that the policies exist and values are set as described in this procedure. If they do not exist, create them using the steps in this procedure. The steps apply only to a VxBlock System with a Cisco UCS Ethernet Adapter Policy for compute Cisco UCS B-Series Blade Servers running VMware ESXi. A service-profile that is associated with the respective compute blades uses the policy.

Steps

1. From the UCS Manager, select **Servers**.
2. Select **Policies** > **root** > **Adapter Policies**.
3. Select **Add a new Ethernet Adapter Policy** to provide a name and description (for example: VMQ-Default).
4. Under **Resources**, enter the following settings:
   - **Transmit Queues = 8** (The number of transmit queue resources to allocate.)
   - **Receive Queues = 4** (The number of receive queue resources to allocate.)
   - **Completion Queues = 12** (The number of completion queue resources to allocate. In general, allocate the number of completion queue resources equal to the number of transmit queue resources plus the number of receive queue resources.)
   - **Interrupts = 14**
5. Under **Options**, select **Enabled** for **Receive Side Scaling (RSS)**. All other values remain as default.

Create the VMQ connection configuration settings

Verify that the VMQ policies exist. If not, create them using the steps in this procedure.

Steps

1. In the **UCSM Navigation** window, click **LAN**.
2. Expand **LAN** > **Policies**.

3. Expand the node for the organization where you want to create the policy.

4. If the system does not include multitenancy, expand the root node.

5. Right-click the **VMQ Connection Policies** node and select **Create VMQ Connection Policy**.

6. In the **Create VMQ Connection Policy** dialog box, complete the following fields:
   - **Name field**: The VMQ connection policy name
   - **Number of VMQs: 16** (The number of VMQs per adapter must be one more than the maximum number of VM NICs)
   - **Number of Interrupts: 34** (The number of CPU threads or logical processors available in the server)

7. Click **OK**.

Assign a virtualization preference to a vNIC

Assign the VMQ connection policy to a vNIC.

Steps

1. In the **UCSM Navigation** window, click **Servers**.

2. On the **Servers** tab, expand **Servers** > **target service profile** > **root** > **vNICs**.

3. Select the **vNIC** name.

4. In the **Connection Policies** section, click **VMQ** and select the **VMQ Connection Policy** from the drop-down.
   In the **Properties** area, the **Virtualization Preference** for the vNIC changes to **VMQ**.

Review system security

Ensure that the Converged Systems adheres to established security settings.

The upgrade does not change security for Converged Systems.

See the following links for important security considerations:
- *Status of TLSv1.1/1.2 Enablement and TLSv1.0 Disablement across VMware products* : https://kb.vmware.com/s/article/2145796
- *Managing TLS Protocol Configuration with the TLS Configurator Utility*: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-82028A21-8AB5-4E2E-90B8-A01D1FAD77B1.html

VMware vSphere 6.7 disables the TLS 1.0 and TLS 1.1 protocols for improved security.

(i) **NOTE:** Some applications only support the older protocols. To revert to the less secure TLS 1.0 and TLS 1.1 protocols, run the TLS Reconfigurator tool.

To run the tool, go the following locations:
- vCenter Server Appliance: **/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator**
- vCenter Server on Windows: **%VMWARE_CIS_HOME%\TlsReconfigurator\VcTlsReconfigurator**

See the following KB article for more information: https://kb.vmware.com/kb/2147469

For security issues related to speculative execution in Intel processors, see https://kb.vmware.com/s/article/55806.

For a description of those security issues, see the following:
- *CVE-2018-3646 (L1 Terminal Fault - VMM)*
- *CVE-2018-3620 (L1 Terminal Fault - OS)*

Remove the old management VMs

Power off and remove the VMs that are no longer needed.

Steps

1. Power off the Windows database server and Windows VUM and remove the following powered off management VMs from the vCenter:
   - vCSA/VMware vCenter

- PSCs
- Database
- VUM

2. Rename PSCs and vCenter vCSA from their temporary name to permanent names in VMware vSphere HTML5 client.

Update AMP VAPP and DRS rules

Update AMP VAPP and DRS rules. The task is not applicable for AMP-2P.

Prerequisites

- Verify the PSCs and vCSA were renamed from their temporary name to permanent names in the VMware vSphere HTML5 client.
- Update the AMP VAPP and DRS rules.
- Update the VAPP and power on settings to include the following:
  - New PSCs
  - New vCSAs
  - NSX Managers
  - New VMs

  Update the AMP DRS rules for the new VMs.

Steps

1. Add VMs PSC1, PSC2, and vCSA into the resource pool. If the resource pool exists, you may move the VMs there. If not, create a resource pool and move the VMs. Follow the steps to move the VMs:
   a. Right-click the VMs **PSC1**, **PSC2**, and **VC01**. Select **Move To…**
   b. At the **Move To…** pane, expand the Datacenter, Hosts and Clusters, AMP-CORE cluster, and Local Management Workload resource pools.
   c. Highlight the new resource pool (for example **Local Management Workload)** and click **OK**.
2. From the HTML5 client, select **AMP-Core Cluster**, and then select the **Configure** tab. Under the **Configuration** sub menu, select **VM/Host Rules** and edit with the following information:

Name	Type	Members
PSC1-PSC2_SVM	Separate Virtual Machines	PSC1 PSC2
PSC1-VC01_KVM	Keep Virtual Machines Together	PSC1 VC01

   a. Select **VM/Host Groups** and edit the virtual machine and host groups with the following information:

Name	Type	Members
v01234PSC1	VM Group	PSC1
v01234VC01	VM Group	VC01

   b. Select **VM/Host Rules** and edit the DRS rules to create host affinity with the following information:

Group Name	Type	Members
VC01_PSC_VMTVM	Virtual Machines To Virtual Machines	First restart the VMs in VM group: VM Group: v01234PSC1 Then restart the VMs in VM group: VM Group: v01234VC01

Group Name	Type	Members
		ⓘ **NOTE:** In the examples, `01234` represents the last 5 digits of the VxBlock System serial number.

3. For AMP-VX, edit the **VM/Host Rules** with the following information:

Name	Type	Members
M01AMXVC-VCProd01_SVM (VMware vSphere 6.5)	Separate VMs	M01VCSA01 V01VCProd01
V01VCprod01_V01PSC01_SVM	Separate VMs	V01VCprod01 V01PSC01
V01VCprod02_V01PSC02_SVM	Separate VMs	V01VCprod02 V01PSC02
V01VCprod03_V01PSC03_SVM	Separate VMs	V01VCprod03 V01PSC03
V01VCprod04_V01PSC04_SVM	Separate VMs	V01VCprod04 V01PSC04
V01VCprod05_V01PSC01_SVM	Separate VMs	V01VCprod05 V01PSC01
V01VCprod06_V01PSC02_SVM	Separate VMs	V01VCprod06 V01PSC02
V01VCprod07_V01PSC03_SVM	Separate VMs	V01VCprod07 V01PSC03
V01VCprod08_V01PSC04_SVM	Separate VMs	V01VCprod08 V01PSC04
V01PSC01-04_SVM	Separate VMs	V01PSC01 V01PSC02 V01PSC03 V01PSC04

a. Select **VM/Host Groups** and edit the virtual machine and host groups with the following information:

Name	Type	Members
V01PSC01	VM Group	V01PSC01
V01VCprod01	VM Group	V01VCprod01
V01PSC01-05	VM Group	V01PSC01 V01PSC02 V01PSC03 V01PSC04 V01PSC05

Name	Type	Members
V01VCprod01-08	VM Group	V01VCprod01 V01VCprod02 V01VCprod03 V01VCprod04 V01VCprod05 V01VCprod06 V01VCprod07 V01VCprod08

b. Select **VM/Host Rules** and edit the DRS rules to create host affinity with the following information:

Group Name	Type	Members
V01PSC_V01VC01_VMTVM	VMs to VMs	First restart VMs in VM group: VM Group: V01PSC1 Then restart VMs in VM group: VM Group: V01VCprod01
V01PSCs-vCenters	VMs to VMs	First restart VMs in the VM Group: V01PSC01-05 Then restart VMs in the VM Group: V01VCprod01-08

Validate folders for AMP-VX

Validate that the folder hierarchy is created for the placement of the VMs for the AMP-VX.

Steps

1. Log in to the management VMware vCenter using the VMware vSphere HTML5 client.
2. Select **VMs and Templates** tab.
3. Verify the following folder structure:
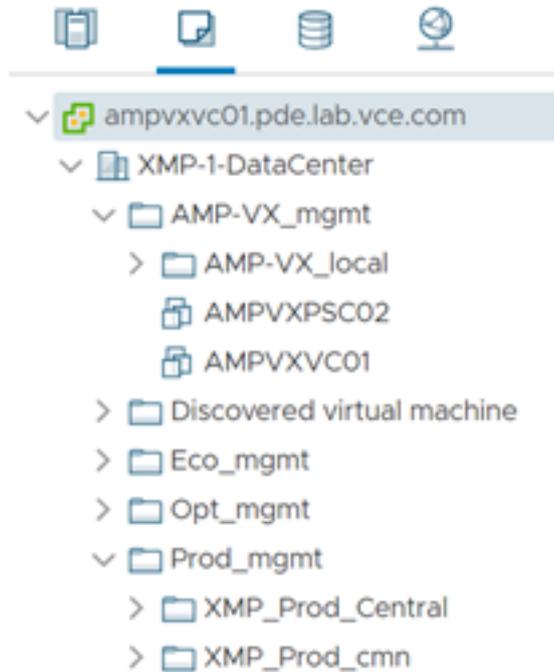
4. Edit the placement using the following information:

Host/VM	Primary folder	Secondary folder	Subfolder
M01PSC01 or LCS equivalent	AMP-VX_mgmt	NA	NA
M02PSC02 or LCS equivalent	AMP-VX_mgmt	NA	NA
M01VCSA01 or LCS equivalent	AMP-VX_mgmt	NA	NA
VxBlock 1000 V01PSC01	PROD_mgmt	XMP_PROD_central	XMP_prod01
VxBlock 1000 V01PSC02	PROD_mgmt	XMP_PROD_central	XMP_prod01
VxBlock 1000 V01VCProd01	PROD_mgmt	XMP_PROD_central	XMP_prod01

Perform a full backup of the system

After the VMware vSphere environment successfully upgrades, back up all VMware vSphere components. See the respective *Administration Guide* for your Converged System.

Update compute VM VMware tools and virtual hardware version

Upgrade the VMware tools and virtual hardware version on the compute VM.

About this task

Perform this task during an application maintenance window, because it requires powering off and rebooting the VM. When the upgrade is complete, power on the VM.

ⓘ **NOTE:** Before upgrading, back up each of the VMs.

Steps

1. Upgrade the VMware tools for the management VMs with Microsoft Windows Server operating system (compute VMs).

   See the *Upgrade Virtual Machines and VMware Tools* procedure in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.update_manager.doc/GUID-0B9FF31B-3702-4BD2-B925-9DAC98051338.html

2. Upgrade the VM hardware to Version 14 for the management VMs with Microsoft Windows Server operating system (compute VMs).

   See the *Upgrade the Compatibility of a Virtual Machine Manually* procedure in the *VMware vSphere Upgrade* documentation: https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.vm_admin.doc/GUID-60768C2F-72E1-42E0-8A17-CA76849F2950.html